Week 6 – Web Application Firewall (WAF) Setup.

Name- Samruddhi Dattu Nikam

PRN- 2124UCSF2019

Email Id- samruddhi.nikam_24ucs@sanjivani.edu.in

Task- 1) Configure Cloudflare or AWS WAF.
2) Protect against OWASP Top 10 attacks.
3) Upload configuration screenshots.

Step 1: Log in to AWS Console

1. Open AWS Management Console.
2. Sign in with your AWS account credentials.

Step 2: Open AWS WAF Service

1. In the search bar, type **WAF & Shield**.
2. Click on **WAF & Shield** service.

Step 3: Create a Web ACL

1. Click **Create Web ACL**.
2. **Name:** Give a descriptive name (e.g., `MyWebACL-OWASP`).
3. **Resource type:** Choose the resource you want to protect (CloudFront, API Gateway, or Application Load Balancer).
4. Select the specific resource (e.g., your CloudFront distribution or ALB).
5. Click **Next**.

Step 4: Add AWS Managed Rules for OWASP Top 10

1. In **Add rules and rule groups**, click **Add managed rule groups**.
2. Select **AWS Managed Rules**.
3. Check **AWSManagedRulesCommonRuleSet** — protects against common OWASP Top 10 attacks like SQL injection, XSS, etc.
4. (Optional) Add other relevant managed rules:
    - **AWSManagedRulesKnownBadInputsRuleSet**
    - **AWSManagedRulesSQLiRuleSet**
    - **AWSManagedRulesLinuxRuleSet** (if applicable)
5. Click **Add rules**.

Step 5: Set Rule Action

Week 6 – Web Application Firewall (WAF) Setup.

1. Leave the default action as **Block** for malicious requests.
2. Click **Next**.

Step 6: Set Default Web ACL Action

1. Choose **Allow** for requests that do not match any rules.
2. Click **Next**.

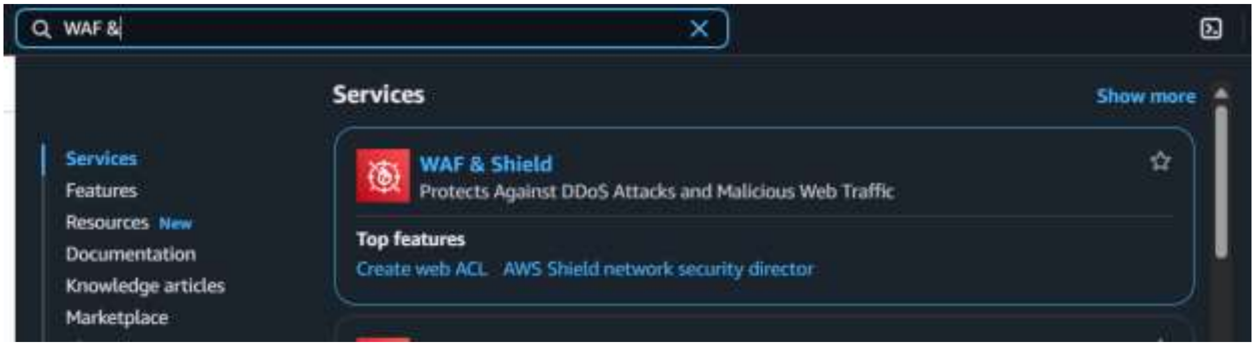
Step 7: Review and Create

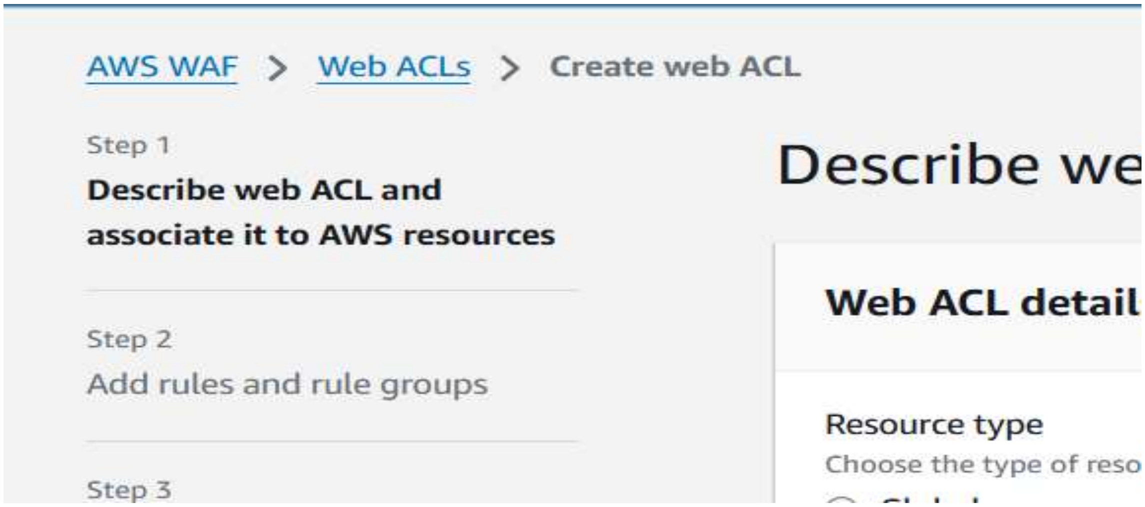
1. Review your settings.
2. Click **Create Web ACL**.

Step 8: Verify

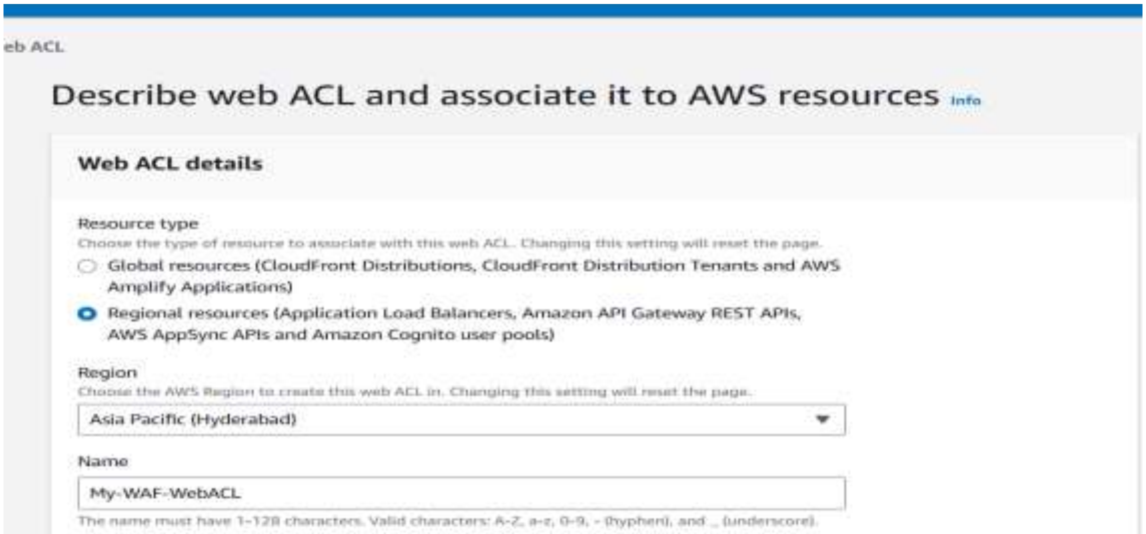
1. Go to the **AWS WAF Dashboard**.
2. Ensure your Web ACL is **Associated** with your resource.
3. Check request metrics to confirm blocking of malicious requests.

❖ Screenshot




AWS WAF > Web ACLs > Create web ACL
Step 1
Describe web ACL and associate it to AWS resources
Step 2
Add rules and rule groups
Step 3
Describe we
Web ACL detail
Resource type
Choose the type of reso

Week 6 – Web Application Firewall (WAF) Setup.



eb ACL

Describe web ACL and associate it to AWS resources Info

Web ACL details

Resource type

Choose the type of resource to associate with this web ACL. Changing this setting will reset the page.

○ Global resources (CloudFront Distributions, CloudFront Distribution Tenants and AWS Amplify Applications)

● Regional resources (Application Load Balancers, Amazon API Gateway REST APIs, AWS AppSync APIs and Amazon Cognito user pools)

Region

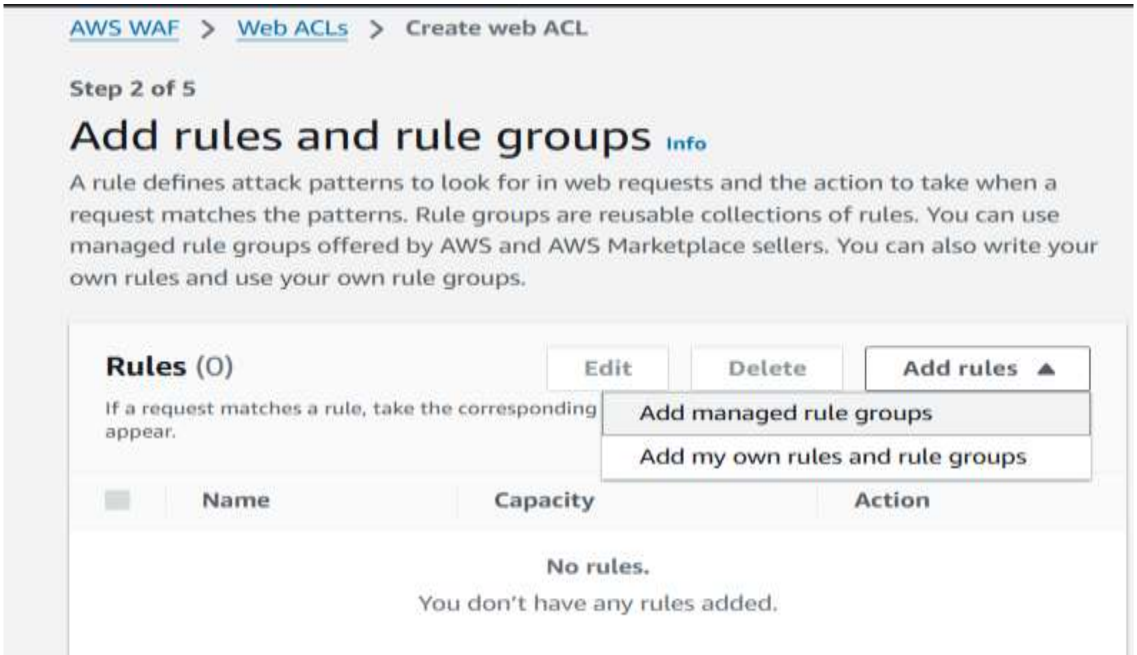
Choose the AWS Region to create this web ACL in. Changing this setting will reset the page.

Asia Pacific (Hyderabad)

Name

My-WAF-WebACL

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).



AWS WAF > Web ACLs > Create web ACL

Step 2 of 5

Add rules and rule groups Info

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

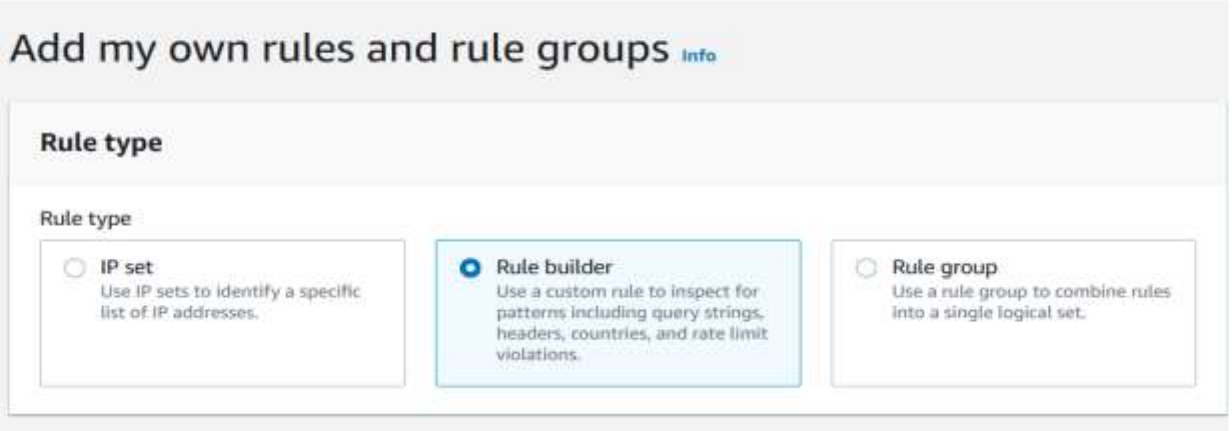
Rules (0)

If a request matches a rule, take the corresponding appear.

□	Name	Capacity	Action

No rules.

You don't have any rules added.



Add my own rules and rule groups Info

Rule type

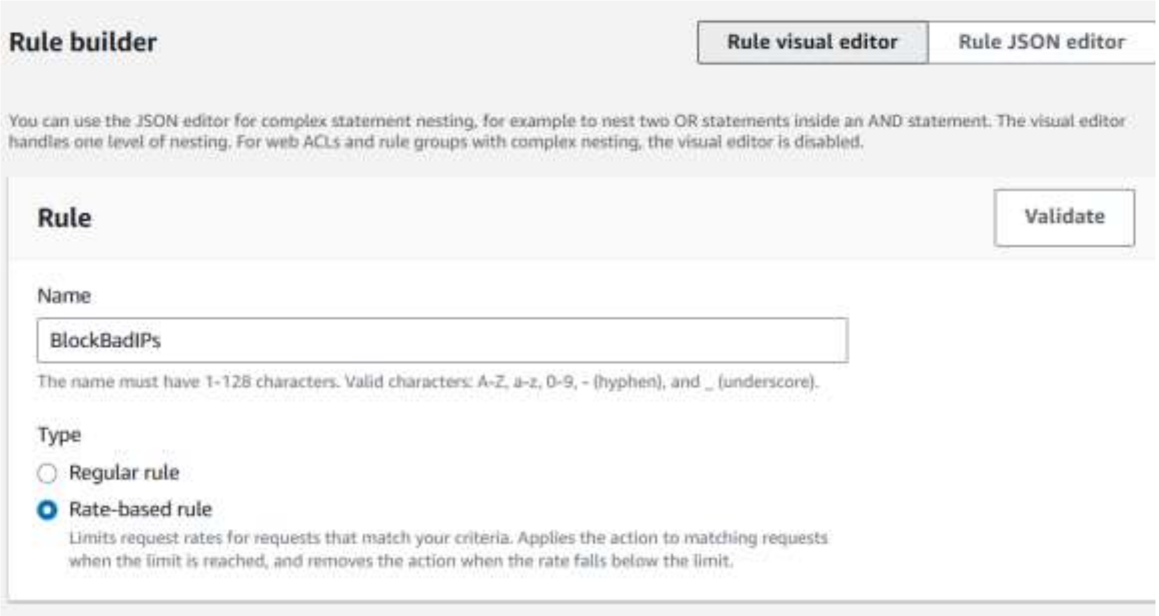
Rule type

○ IP set
Use IP sets to identify a specific list of IP addresses.

● Rule builder
Use a custom rule to inspect for patterns including query strings, headers, countries, and rate limit violations.

○ Rule group
Use a rule group to combine rules into a single logical set.

Week 6 – Web Application Firewall (WAF) Setup.



Rule builder

You can use the JSON editor for complex statement nesting, for example to nest two OR statements inside an AND statement. The visual editor handles one level of nesting. For web ACLs and rule groups with complex nesting, the visual editor is disabled.

Rule

Name

BlockBadIPs

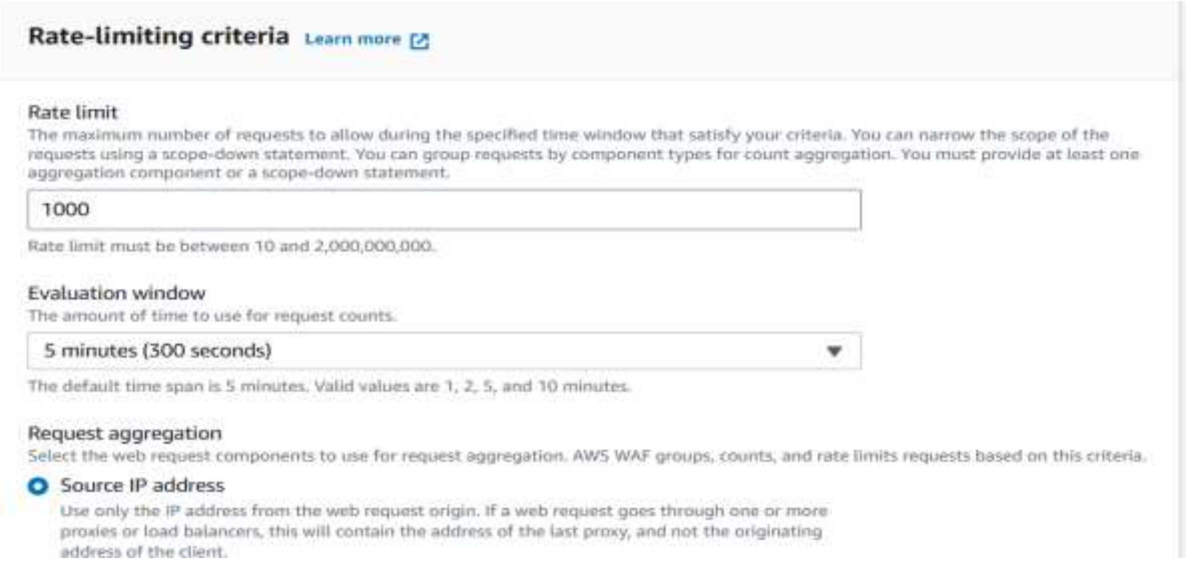
The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

Type

○ Regular rule

● Rate-based rule

Limits request rates for requests that match your criteria. Applies the action to matching requests when the limit is reached, and removes the action when the rate falls below the limit.



Rate-limiting criteria

Rate limit

The maximum number of requests to allow during the specified time window that satisfy your criteria. You can narrow the scope of the requests using a scope-down statement. You can group requests by component types for count aggregation. You must provide at least one aggregation component or a scope-down statement.

1000

Rate limit must be between 10 and 2,000,000,000.

Evaluation window

The amount of time to use for request counts.

5 minutes (300 seconds) ▼

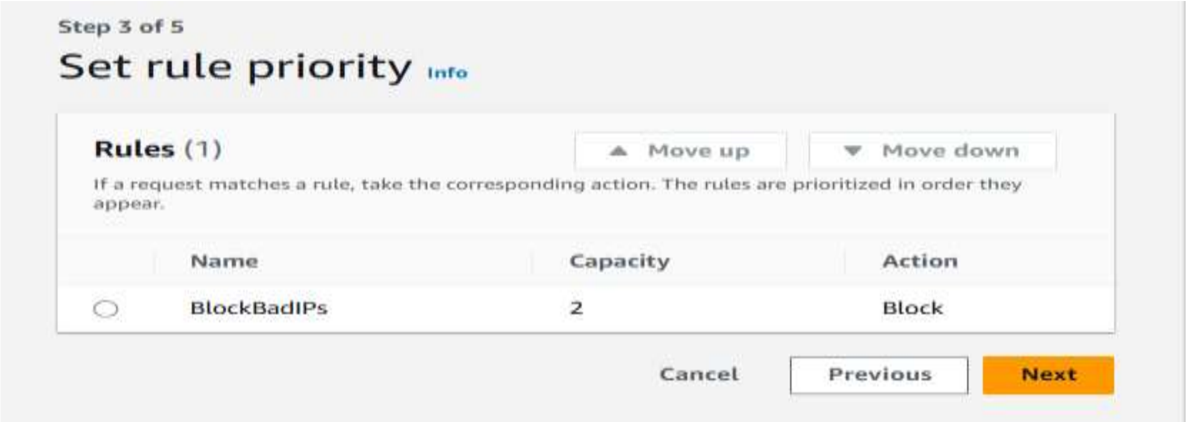
The default time span is 5 minutes. Valid values are 1, 2, 5, and 10 minutes.

Request aggregation

Select the web request components to use for request aggregation. AWS WAF groups, counts, and rate limits requests based on this criteria.

● Source IP address

Use only the IP address from the web request origin. If a web request goes through one or more proxies or load balancers, this will contain the address of the last proxy, and not the originating address of the client.



Step 3 of 5

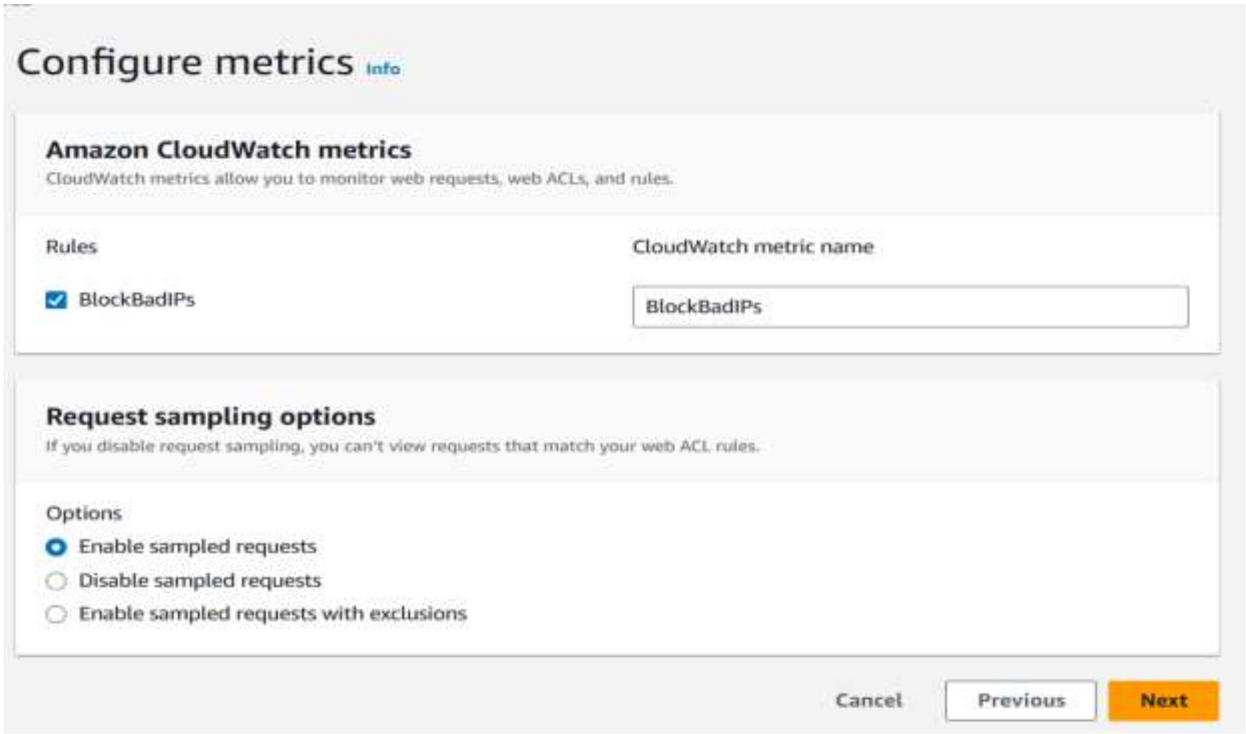
Set rule priority

Rules (1)

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

	Name	Capacity	Action
○	BlockBadIPs	2	Block

Week 6 – Web Application Firewall (WAF) Setup.



Configure metrics Info

Amazon CloudWatch metrics

CloudWatch metrics allow you to monitor web requests, web ACLs, and rules.

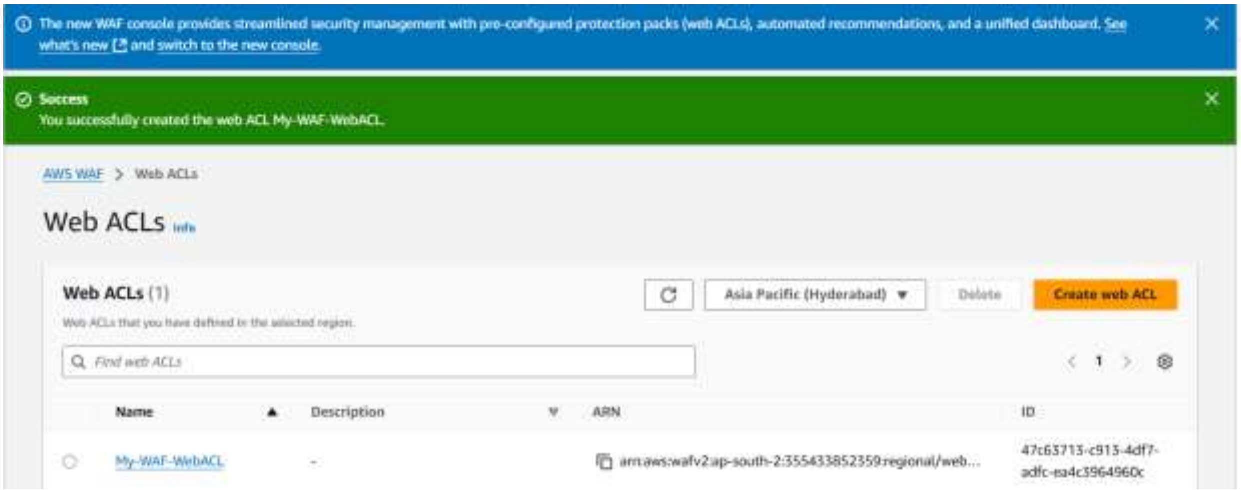
Rules	CloudWatch metric name
☑ BlockBadIPs	BlockBadIPs

Request sampling options

If you disable request sampling, you can't view requests that match your web ACL rules.

Options

● Enable sampled requests
○ Disable sampled requests
○ Enable sampled requests with exclusions



The new WAF console provides streamlined security management with pre-configured protection packs (web ACLs), automated recommendations, and a unified dashboard. See what's new and switch to the new console.

Success
You successfully created the web ACL My-WAF-WebACL.

Web ACLs Info

Web ACLs (1)

Web ACLs that you have defined in the selected region.

	Name	Description	ARN	ID
○	My-WAF-WebACL	-	arn:aws:wafv2:ap-south-2:355433852359:regional/web...	47c63713-c913-4df7-adfc-ea4c3964960c